**INFORMACIÓN PRINCIPAL**

Título: Sistema de telemetría Mi Monitor

Nombre del establecimiento: {{nombre\_establecimiento}}

Dirección del establecimiento: {{direccion\_establecimiento}}

Informe de validación: N° 3

Fecha calificación: 02/07/2025

**OBJETIVO**

Evidenciar documentalmente la correcta aplicación del sistema de telemetría en el monitoreo de las condiciones de temperatura en la cadena de frío y condiciones ambientales de {{nombre\_establecimiento}} validando su sistema informático para el registro de datos y poder así garantizar el cumplimiento de las condiciones establecidas en el protocolo.

**ALCANCE**

Dar cumplimiento con los requisitos de funcionamiento de la plataforma del sistema de telemetría, modelada para satisfacer las necesidades del entorno. Como se trata de un solo sistema en todos los procesos, se validará su funcionamiento de manera general, y se especificará con evidencias fotográficas el 10% de los equipos que monitoreen medicamentos. Esta validación se realizará cada 2 años.

# RESPONSABILIDADES

* Personal de Netux: Realizará la calificación y registrará la información acorde al protocolo.
* Profesional Mantenimiento del servicio: Supervisará las actividades y verificará que los registros estén completos.
* Ingeniero Netux: Realizará informe de calificación de diseño. Redactará e informará de desviaciones presentadas.
* Profesional Mantenimiento del servicio: aprobará el informe de calificación de diseño.
* Dirección Técnica del servicio: dará el visto bueno al informe de calificación de diseño.

|  |  |
| --- | --- |
| **PREGUNTAS EVALUACIÓN DE IMPACTO** | **SI/NO** |
| 1. ¿El sistema informatizado se utiliza para aprobar o rechazar un producto? | **SI** |
| 2. ¿El sistema informatizado o hardware posee in firmware que modifique su procesamiento lógico? | **NO** |
| 3. ¿El sistema informatizado o hardware posee un controlador lógico programable (PLC) | **NO** |
| 4. ¿El sistema es usado para la toma de decisiones con un impacto en calidad, regulatorio o GxP? | **NO** |
| 5. ¿El sistema genera reporte de datos regulatorios, reportes de análisis, certificados o decisiones de calidad de los productos? | **SI** |
| 6. ¿El sistema contiene información de la trazabilidad hacia adelante o hacia atrás de los productos? | **SI** |
| 7. ¿El sistema es usado para el control de documentación del sistema de gestión de calidad o documentación de manufactura? | **NO** |
| 8. ¿El sistema es usado para el control de cualquier empaque o actividad de etiquetado ó rotulado? | **NO** |
| 9. ¿El sistema se usa para rastrear/realizar mantenimiento y/o pruebas de calibración, laboratorio, equipos de producción o manufactura? | **NO** |
| 10. ¿El sistema se usa para mantenimiento, compras, inventarios o distribución de datos de los productos? | **NO** |
| 11. ¿El sistema tiene, maneja o registra datos críticos como lote, fecha de vencimiento, fecha de manufactura, procesos de control y procesos de análisis? | **NO** |

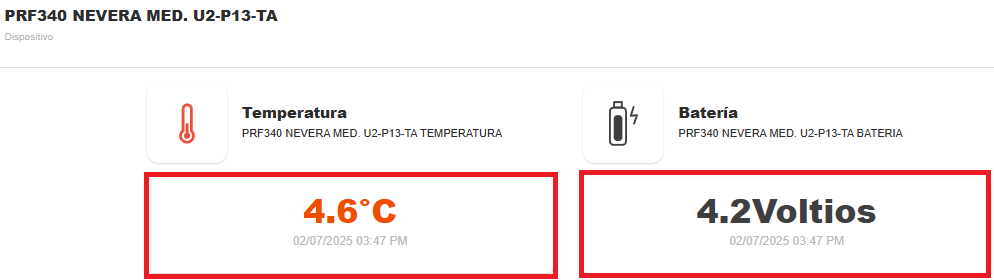
**\*\*Si alguna de las respuestas anteriores obtuvo como resultado (SI) el software genera impacto y debe ser validado.**

**ESPECIFICACIONES FUNCIONALES**

1. **Registro de valores de magnitudes físicas**

Los valores registrados de temperatura de refrigeración, temperatura de congelación, temperatura ambiente, temperatura de ultracongelación, temperatura de Horno, temperatura de Incubadora, Punto de Rocío y Monóxido de Carbono, son tomados y almacenados en la plataforma con su respectiva unidad de medición (°C, F° o ppm)

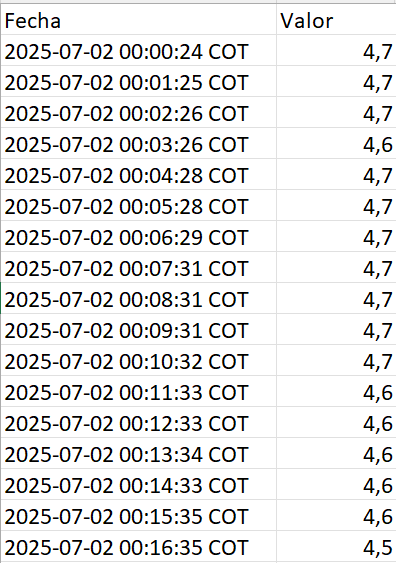
Todos los valores pueden ser consultados en línea.



1. **Registro de datos en tiempo real (la fecha del sistema debe corresponder a la fecha de registro)**

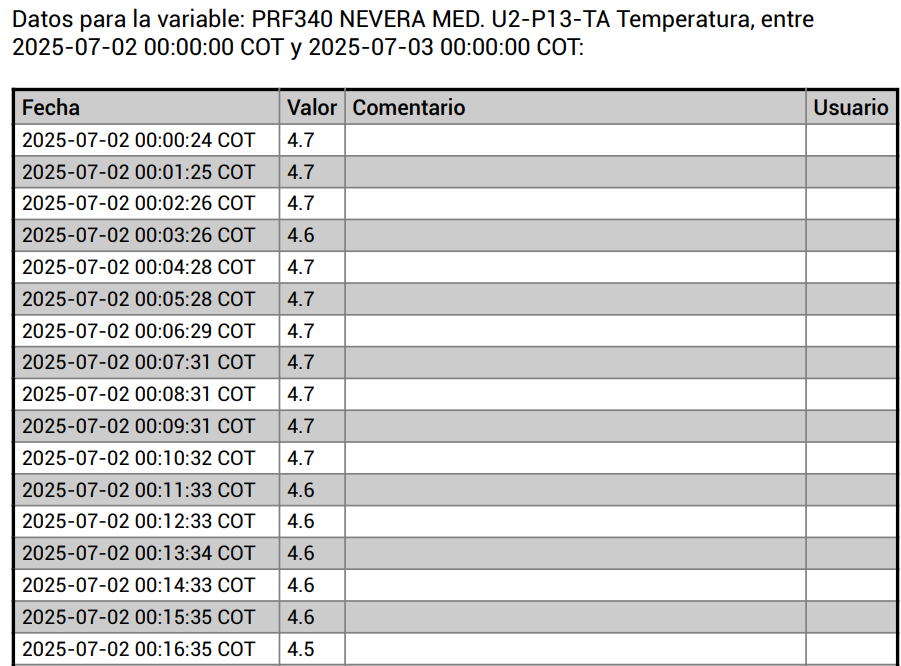
La plataforma de Monitoreo almacena los datos adquiridos bajo el formato DD/MM/YYYY – hh:mm

Este formato se puede verificar en los informes generados por la plataforma en archivo plano Excel



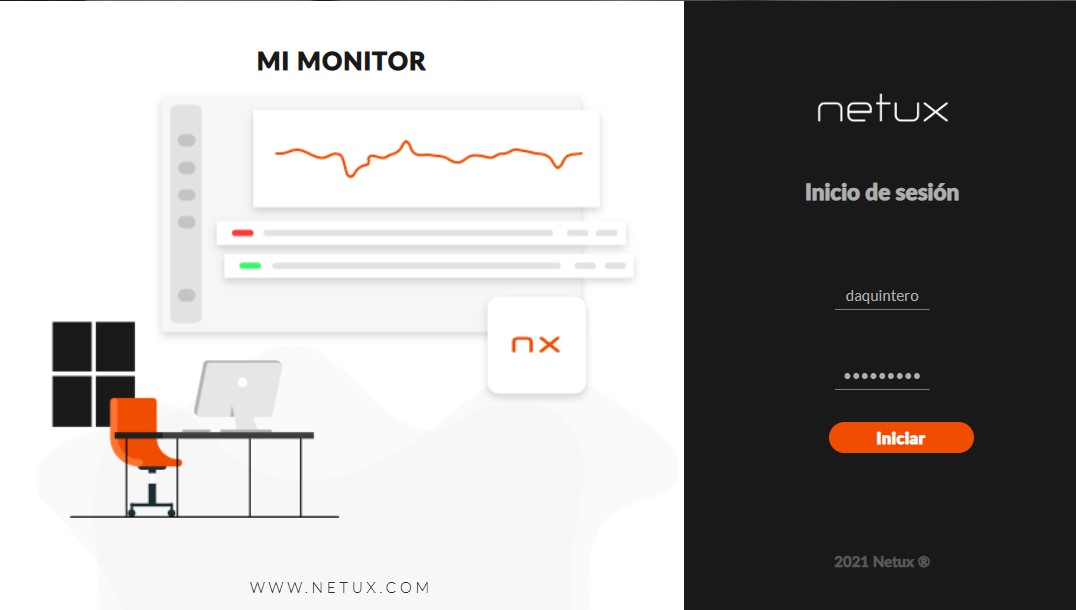
De esta forma el sistema de monitoreo garantiza una continuidad en la toma de datos.

Los archivos se descargan en archivo plano (Excel), también existe la posibilidad de realizar una descarga de información en formato PDF, al ser un archivo inmodificable podrá cumplir con los procesos internos establecidos por la institución.



1. **Autenticación de usuario y contraseña**

El usuario y contraseña es establecido por Netux SAS y debe ser utilizado en la página principal, la autenticación de usuario se basa en dos parámetros y un perfil específico.



En la página de autenticación se debe ingresar el e-mail o usuario suministrado por Netux SAS.

**Perfiles**

La plataforma cuenta con diversos perfiles de visualización y administración de plataforma.

•**Perfil Visualizador:** Este perfil es utilizado por el cliente de la plataforma y entre sus características técnicas solo puede visualizar el estado de las variables y generar informes, la creación de grupos no está disponible para este usuario.

•**Perfil Administrador:** Además de las funciones de visualizador, este perfil puede crear grupos para segmentar los dispositivos y permitir que la información de variables sea vista solo por ciertos visualizadores.

•**Perfil Súper administrador:** Además de las funciones de visualizador y administrador, el perfil súper administrador permite crear las alarmas, las variables y los equipos. Este perfil es de carácter técnico y solo es utilizados por el proveedor del servicio Netux SAS.

El perfil de los usuarios VISUALIZADOR, ADMINISTRADOR Y SUPERADMINISTRADOR depende únicamente del nombre de usuario y su contraseña específica.

Por seguridad el único usuario SUPER-ADMINISTRADOR del sistema es Netux S.A.S. Al usuario VISUALIZADOR Y ADMINISTRADOR se permite perfilar una serie de permisos, para que realice configuraciones básicas en el sistema, esto para evitar que elimine o realice modificaciones críticas que involucren el correcto funcionamiento de registro de información de los dispositivos.

Usuario: daquintero

Contraseña: \*\*\*\*\*\*\*\*\*

|  |  |
| --- | --- |
| VISUAL\_ADMIN | VISUAL\_CLIENT |
| Visualizar variables | Visualizar variables |
| Visualizar variables en tabla | Visualizar variables en tabla |
| Visualizar equipos | Leer comentarios de variables |
| Visualizar organización | Visualizar equipos |
| Visualizar contactos | Leer archivos |
| Visualizar grupos | Visualizar tablero dashboard |
| Visualizar tablero dashboard | Leer reportes |
| Leer reportes | Visualizar grupos |
| Leer comentarios de variables | Crear comentarios en gráfica |
| Leer archivos |  |
| Crear comentarios en gráfica |  |
| Crear grupos |  |
| Crear archivos |  |
| Actualizar grupos |  |

El perfil de los usuarios VISUAL\_CLIENT o VISUAL\_ADMIN depende únicamente del nombre de usuario y su contraseña específica.

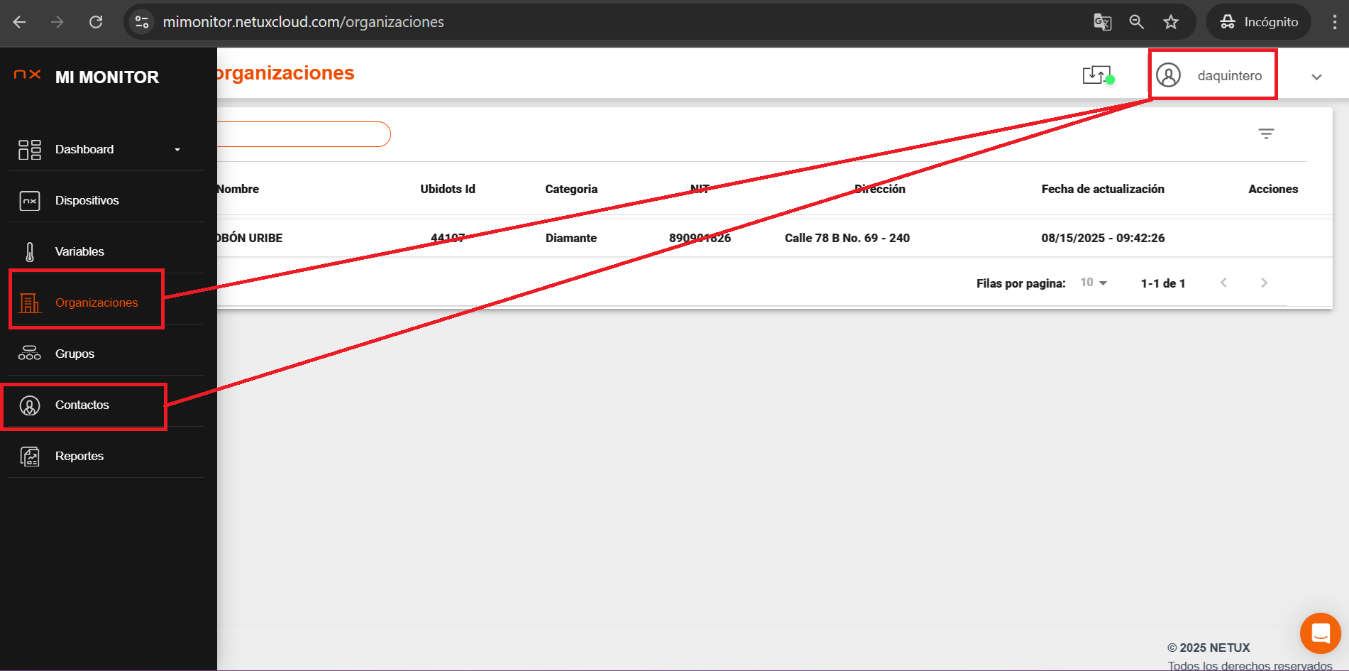
La plataforma de monitoreo ha sido diseñada principalmente como una herramienta de visualización de registros, cuya función esencial es permitir a los usuarios consultar datos históricos y actuales de manera clara, estructurada y accesible. Esta solución tecnológica no permite la modificación de los registros, y los perfiles de usuario disponibles en la plataforma no incluyen privilegios de súper administrador ni capacidades para realizar configuraciones dentro del sistema. En el caso específico de la plataforma Mi Monitor, los roles de usuario están configurados únicamente para la visualización de datos. Esto elimina la necesidad de registrar acciones para auditar cambios, ya que no se pueden realizar modificaciones dentro del sistema. Debido a estas características de diseño orientadas exclusivamente a la consulta de datos, y en ausencia de operaciones que impliquen edición, eliminación o sobrescritura de información, no se considera necesaria la implementación de un sistema de Audit Trail (rastro de auditoría) en esta plataforma. Esta decisión se fundamenta en el principio de proporcionalidad y enfoque basado en riesgo, toda vez que la integridad de los registros se mantiene asegurada mediante controles de acceso y restricciones de funcionalidad adecuadas al nivel de criticidad del sistema.

Cabe resaltar que la plataforma está alineada con el objetivo de garantizar la trazabilidad y disponibilidad de la información, sin comprometer su integridad, y que su diseño cumple con los principios de buenas prácticas de gestión de datos en sistemas informáticos, según los lineamientos de GAMP 5.

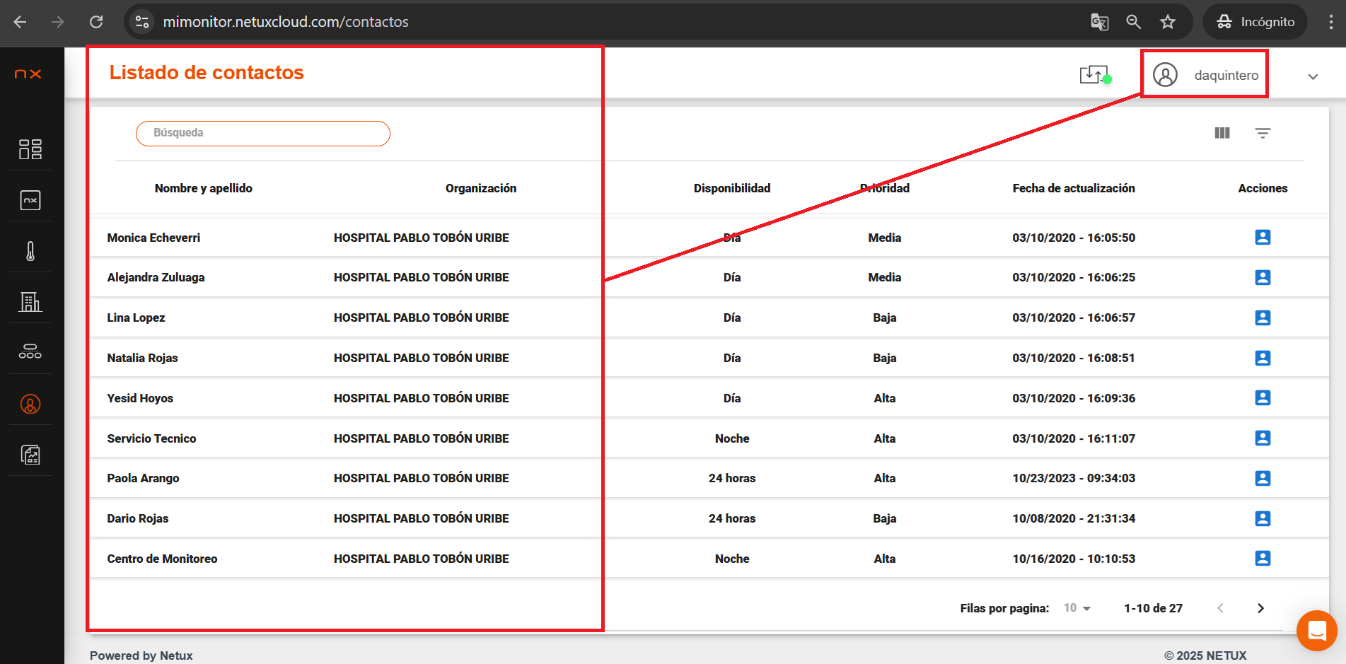
|  |  |
| --- | --- |
| **ADMIN\_CLIENT** | **VISUAL\_CLIENT** |
|  |  |

**Usuario Administrador**

1. **Permite visualizar los módulos de contactos y organizaciones**



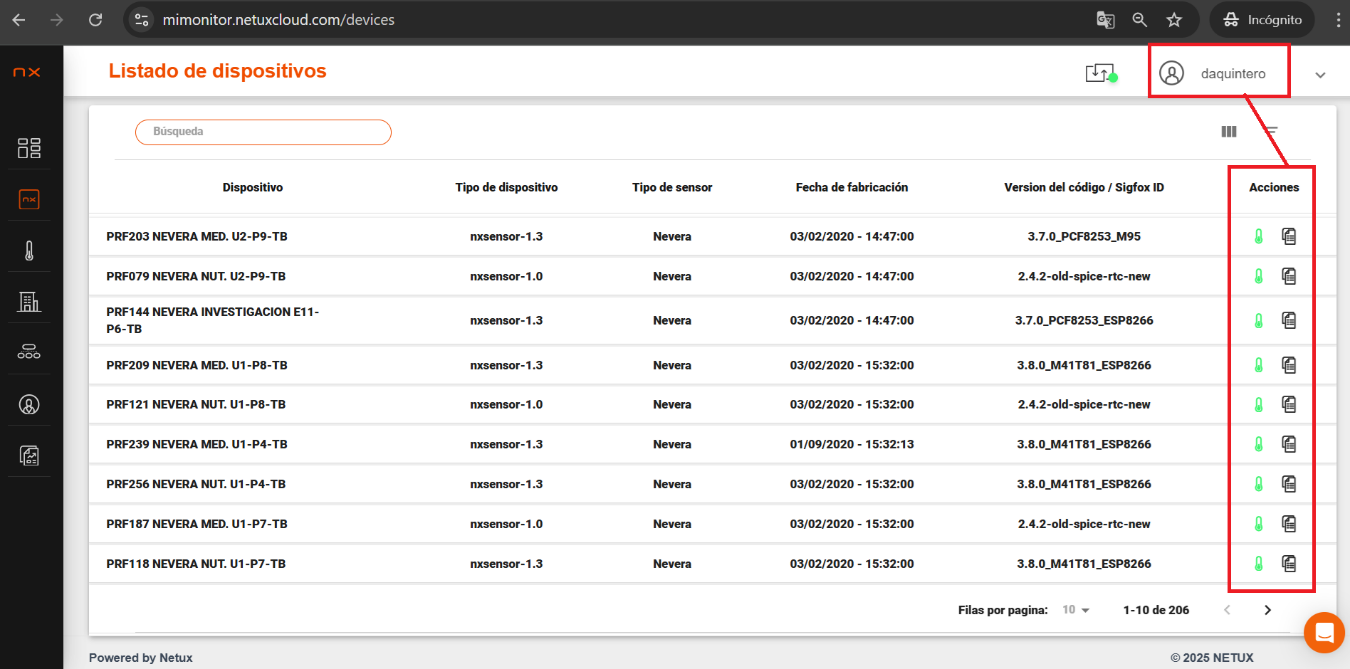
1. **Vista de contactos de la organización**



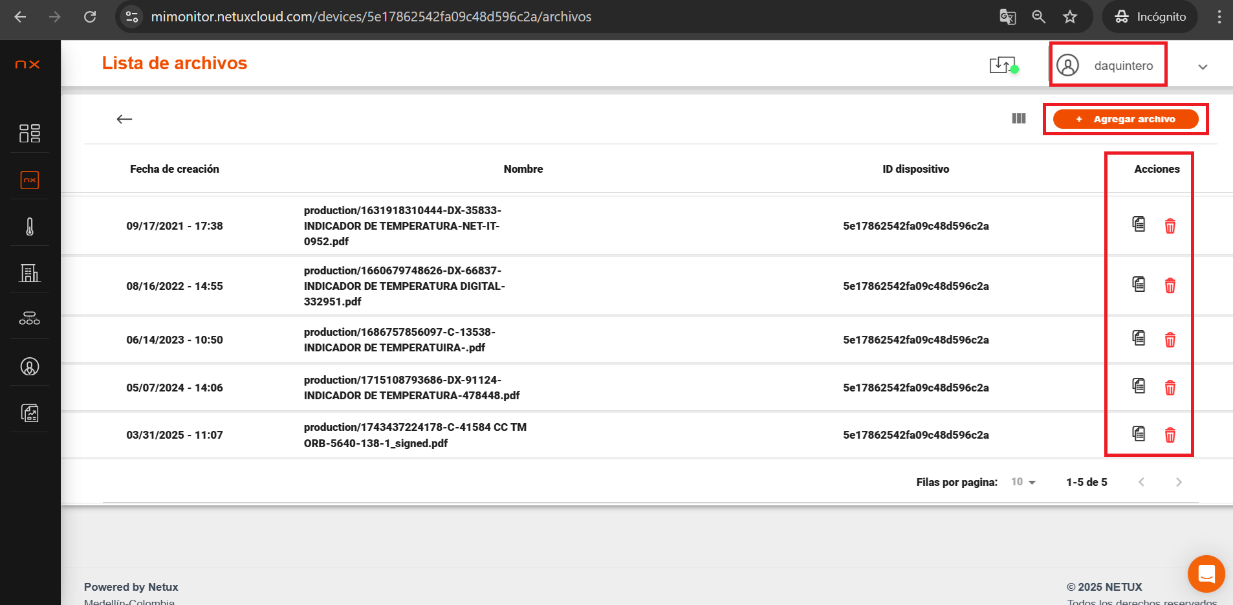
1. **Permite la creación de Grupos y Sedes**

****

1. **Acceso al módulo de Documentos**

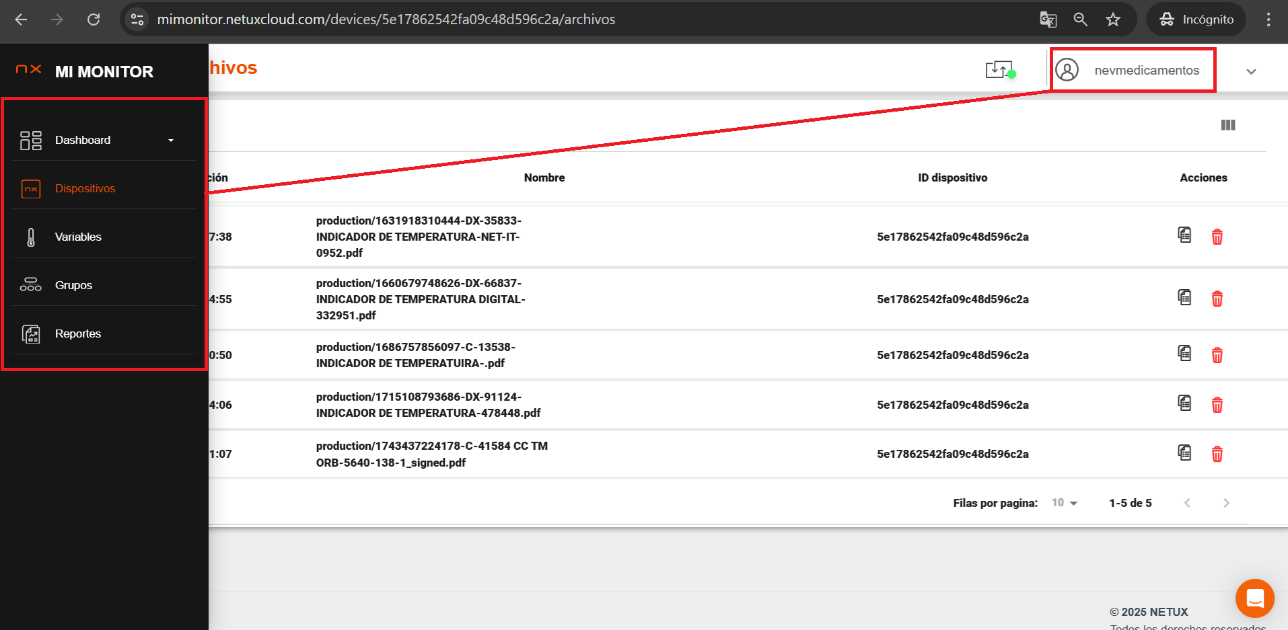
****

1. **Permite agregar archivos**

****

**Usuario cliente:**

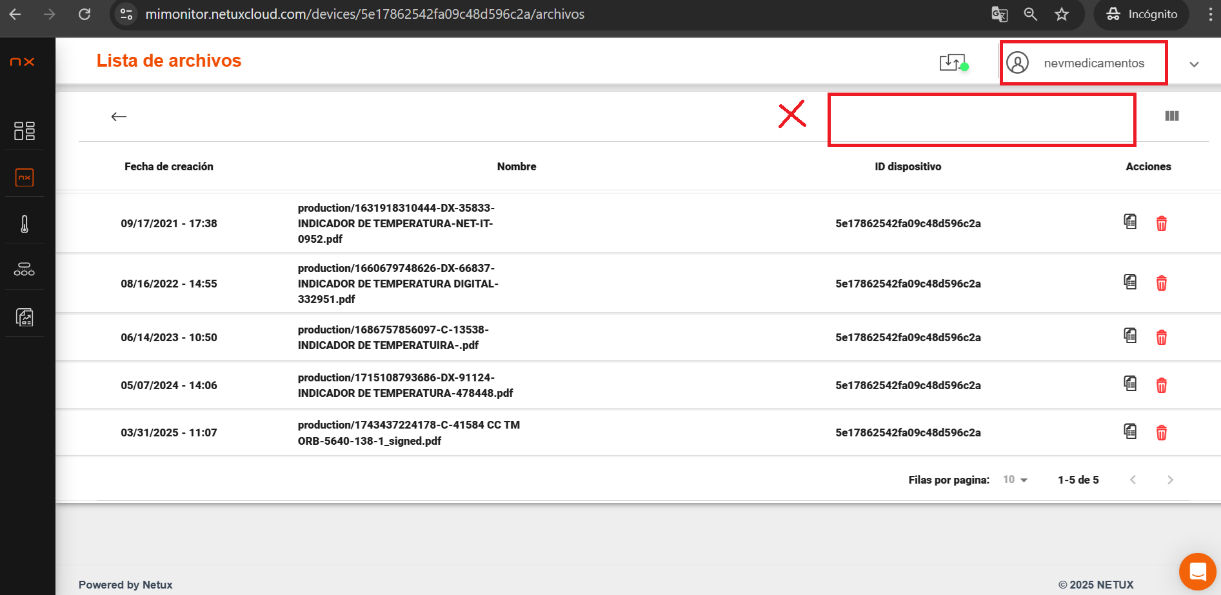
1. **No cuenta con acceso al módulo de Organización y contactos**

****

1. **Sólo es posible la visualización del grupo en el que se encuentra configurado**

****

1. **No es posible agregar archivos**

****

**Seguridad**

El esquema de monitoreo de variables que utiliza Netux S.A.S, posee una arquitectura de red, en donde la información se transmite y se almacena en la nube, a continuación, se muestra una figura que describe la forma transmisión y almacenamiento.

Diagrama

Descripción generada automáticamente

Con la finalidad de brindar a los clientes la seguridad y tranquilidad de que sus datos están protegidos, se mencionan a continuación los protocolos de seguridad que cumple la plataforma:

* SSL
* HTTPS
* AES\_256\_CBC

Estos certificados fueron expedidos por la compañía norte americana STARFIELD SSL CERTIFICATES. http://www.starfieldtech.com/. Esto garantiza que la información que se transmita hacia la plataforma esta encriptada y no sea susceptible de ataques de eavesdropping ó sniffer de red.

HTTPS Hypertext Transfer Protocol Secure (en español: Protocolo seguro de transferencia de hipertexto), más conocido por sus siglas HTTPS, es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP. Es utilizado principalmente por entidades bancarias, tiendas en línea, y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas.

La idea principal de https es la de crear un canal seguro sobre una red insegura. Esto proporciona una protección razonable contra ataques eavesdropping y maninthemiddle, siempre que se empleen métodos de cifrado adecuados y que el certificado del servidor sea verificado y resulte de confianza. La confianza inherente en HTTPS está basada en una Autoridad de certificación superior que viene preinstalada en el software del navegador (Es el equivalente a decir "Confío en la autoridad de certificación, -p.e. VeriSign/Microsoft/etc.- para decirme en quien debería confiar"). Sin embargo, una conexión HTTPS a un website puede ser validada si y solo si todo lo siguiente es verdad:

1. El usuario confía en la Autoridad de certificación para dar fe solo para websites legítimos sin nombres engañosos.
2. El website proporciona un certificado válido (y un certificado inválido muestra una alerta en la mayoría de los navegadores), lo que significa que está firmado por una autoridad confiable.
3. El certificado identifica correctamente al website (p.e. visitando https://algunsitio y recibiendo un certificado para "AlgunSitio S.A." y no "AlgunZitio S.A.").
4. Cada uno de los nodos involucrados en internet son dignos de confianza, o que el usuario confíe en que la capa de cifrado del protocolo (TLS o SSL) es inquebrantable por un eavesdropper.

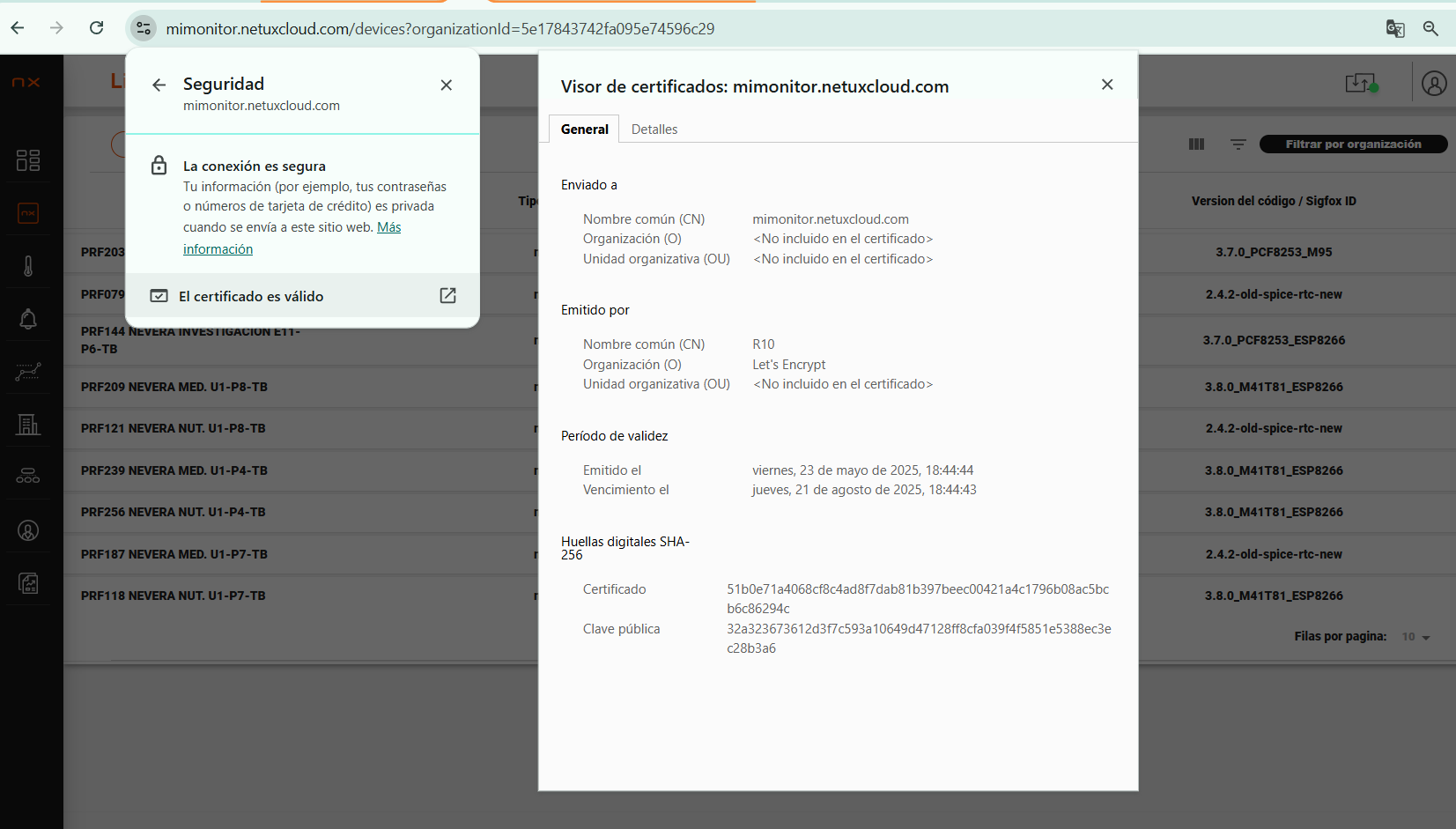
**SSL**

Secure Sockets Layer -Protocolo de Capa de Conexión Segura- (SSL) es un protocolo criptográfico que proporcionan comunicaciones seguras por una red, comúnmente Internet. SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. SSL implica una serie de fases básicas:

**\*\*Negociar entre las partes el algoritmo que se usará en la comunicación**

**\*\*Intercambio de claves públicas y autenticación basada en certificados digitales**

**\*\*Cifrado del tráfico basado en cifrado simétrico**

****

**Visor de certificados en navegador Página mimonitor.netuxcloud.com**

**INTEGRIDAD DE LOS DATOS**

La integridad de los datos o de la información garantiza la exactitud de los datos transportados o almacenados, demostrando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada.

La autenticación basada en tokens se ha convertido en el estándar para la web. API's y Mi Monitor también lo han adoptado como una mejor práctica. La seguridad de los datos radica en que estos son transmitidos con llaves informáticas de 256 bits de longitud (Api\_key) que son renovadas cada minuto o cada dos minutos, esto permite que los datos solo puedan ser visualizados.

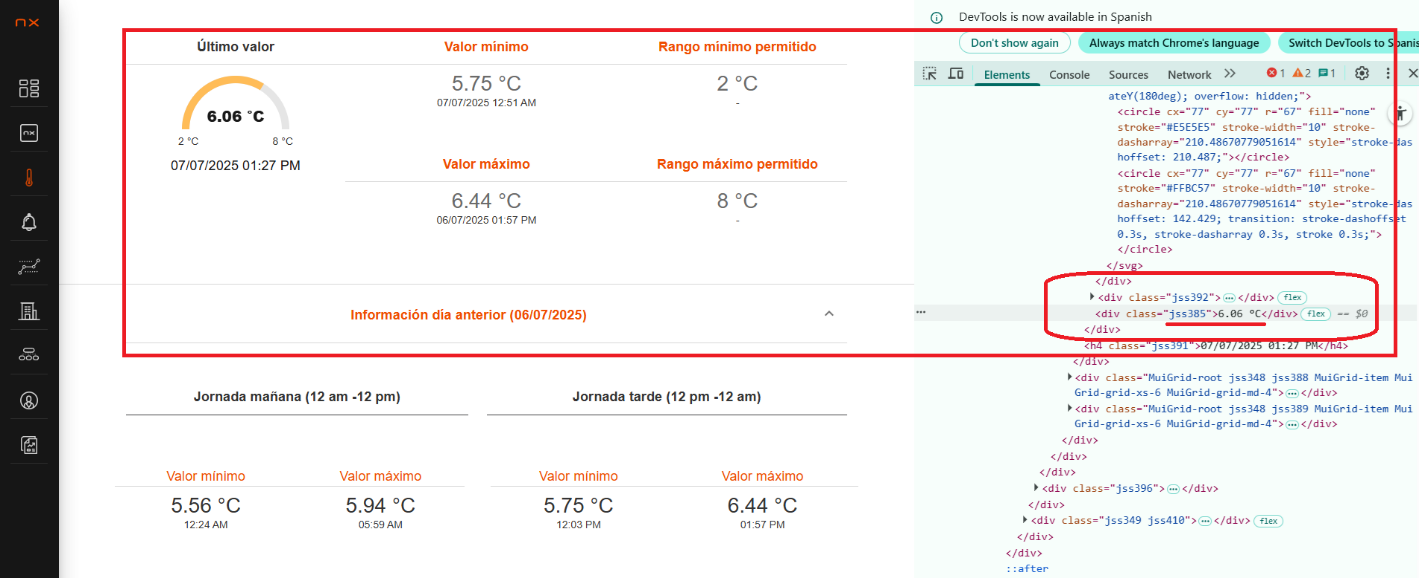
Interfaz de usuario gráfica, Tabla

El contenido generado por IA puede ser incorrecto.

**Mapa de permisos Sistema de telemetría MiMonitor**

Adicionalmente, el diseño arquitectónico del sistema permite el cumplimiento de la Resolución 4410 de 2009 —Manual de Buenas Prácticas de Manufactura de los Gases Medicinales—, la cual establece que “...los parámetros de calidad del aire serán objeto de monitoreo continuo y registro permanente e inmodificable”. En alineación con este requerimiento, la plataforma restringe las acciones del usuario al rol de solo lectura, definido mediante el permiso “CAN\_READ”, exclusivamente para la consulta de variables. Esto asegura que los registros monitoreados sean permanentes, trazables e inalterables.

La única funcionalidad adicional disponible es la posibilidad de registrar comentarios dentro de las gráficas, con el objetivo de documentar, dar seguimiento y controlar las desviaciones detectadas. Esta capacidad no compromete la integridad del dato monitoreado, ya que los comentarios no modifican el valor original registrado, sino que lo complementan dentro del marco de trazabilidad del sistema.

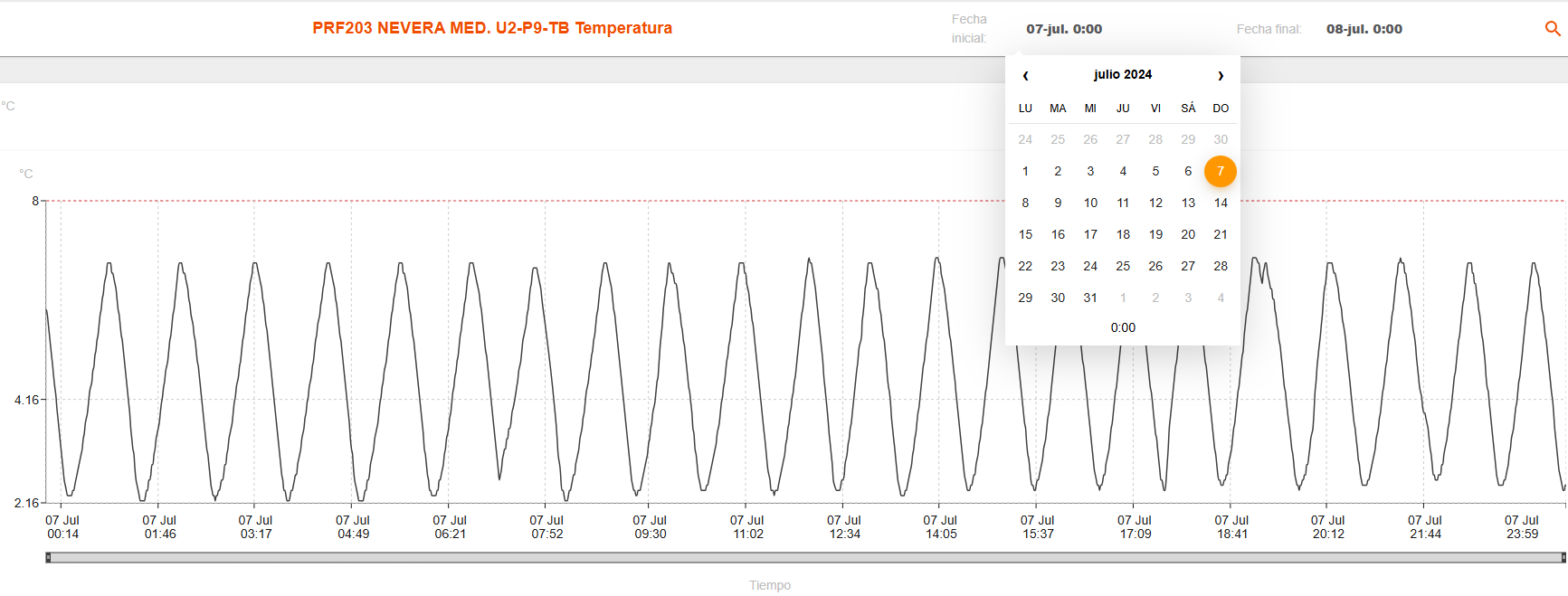


Dentro de la consola de la plataforma web del sistema Mi Monitor, se puede validar que cada que vez que se actualiza un registro o llega un dato nuevo, este se le asigna una clase “jss#” con un número aleatorio asociado al valor, permitiendo que sólo se registre ese valor a la clase correspondiente. Como se puede evidenciar de acuerdo con el diseño, los datos en ninguna circunstancia pueden ser modificados, eliminados o alterados garantizando de esta forma su integridad.

1. **Back up de datos y actualización de registros del sistema**

La plataforma cuenta con la capacidad de mantener en línea hasta un (1) año de información registrada, la cual puede ser consultada en cualquier momento por los usuarios autorizados.

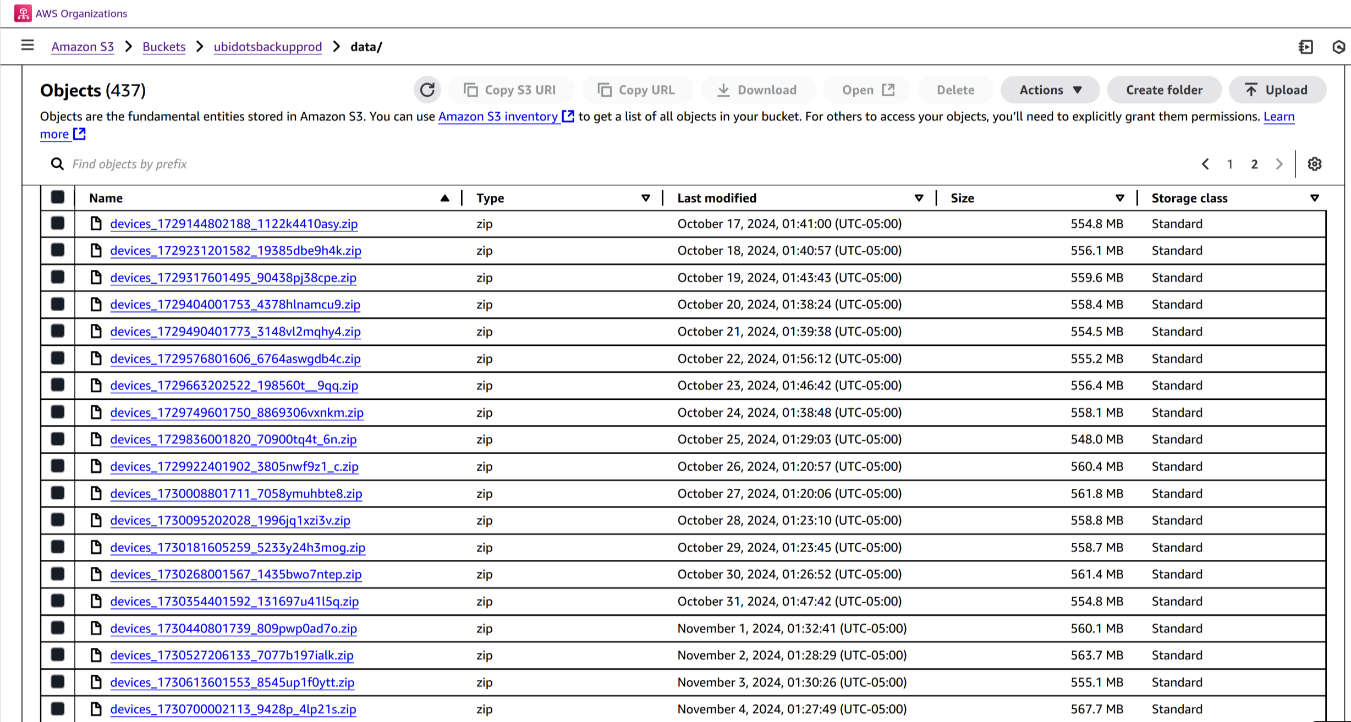
Adicionalmente, el proveedor de infraestructura en la nube, Amazon Web Services (AWS), realiza de forma automática procesos de respaldo (backups), mediante la generación de imágenes o copias de seguridad diferenciadas. Esta funcionalidad garantiza la protección, disponibilidad y recuperación oportuna de la información crítica almacenada, cumpliendo con los estándares de seguridad y continuidad operativa exigidos en entornos regulados.



**Datos en línea del sistema 12 meses atrás (2024)**

De esta manera, tanto los usuarios con permisos de VISUALIZADORES como los ADMINISTRADORES tienen la capacidad de acceder a los datos registrados en la plataforma. Este acceso puede abarcar un lapso de hasta 24 horas en tiempo real o pueden optar por seleccionar un período específico de hasta un año atrás (en periodos de 15 días máximo). Además, les es posible descargar datos correspondientes mes a mes hasta un año atrás

Actualmente, la base de datos de valores de Mi Monitor (No-SQL) tiene un factor de replicación de 3, lo que significa que hay 3 nodos que contienen toda la información en todo momento. Si alguno de los nodos falla, el sistema continuaría operando, usando los otros 2 nodos. La base de datos de valores se respalda cada mes como una medida de seguridad adicional en caso de una interrupción completa de los 3 nodos. Actualmente se está trabajando para garantizar copias de seguridad más periódicas.



1. **Visualización de variables a través de un set de herramientas de visualización e integración con api´s estándar**

La visualización de los datos tiene tres fases:

* **Gráficas**

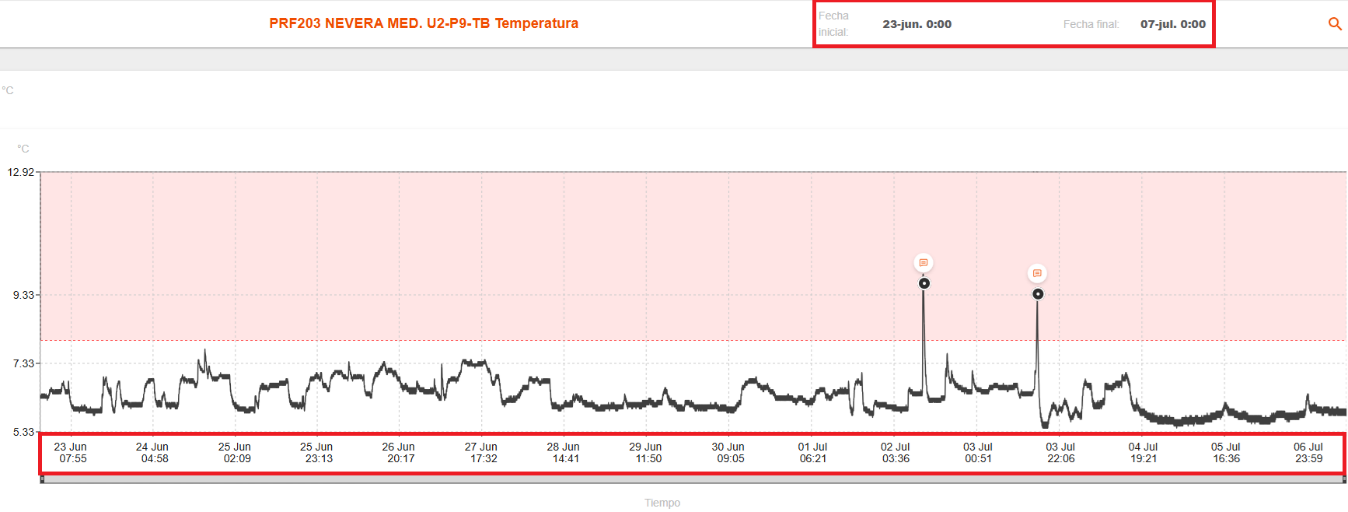
Este ítem es utilizado para verificar el funcionamiento de los equipos en el tiempo y posee diferentes opciones como: ✓ Selección de gráfica por tiempo. Los periodos de tiempo establecidos son:

• 1 día

• 5 días

• 10 días

• 15 días



Además de esto, el tiempo también puede ser seleccionado por el usuario para permitirle navegar a cualquier instante de tiempo, en el que desee visualizar el registro gráfico del sistema

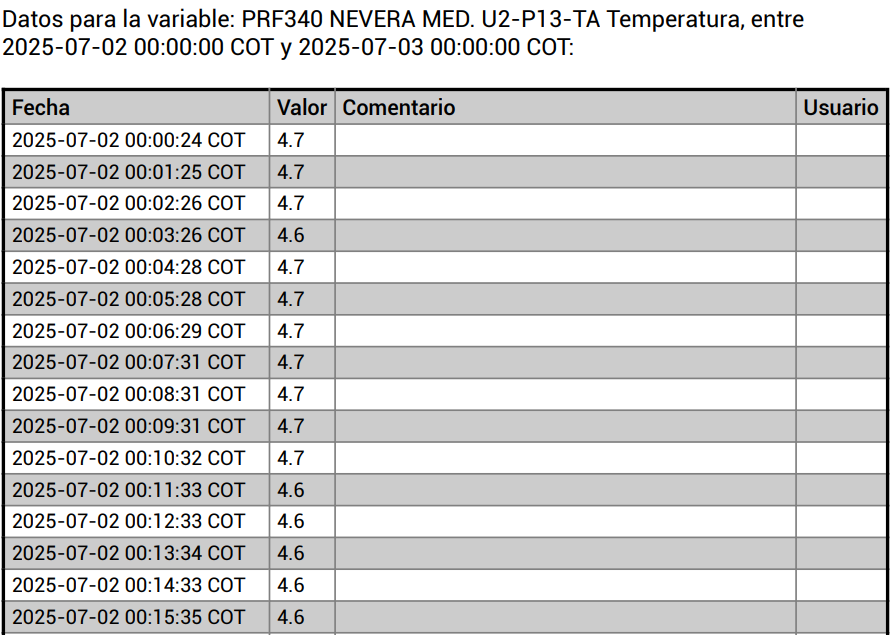
* **Reportes**

Los informes pueden ser consultados de dos formas diferentes en línea o en archivo plano, el cual puede ser consultado por EXCEL o PDF

Tabla

El contenido generado por IA puede ser incorrecto.

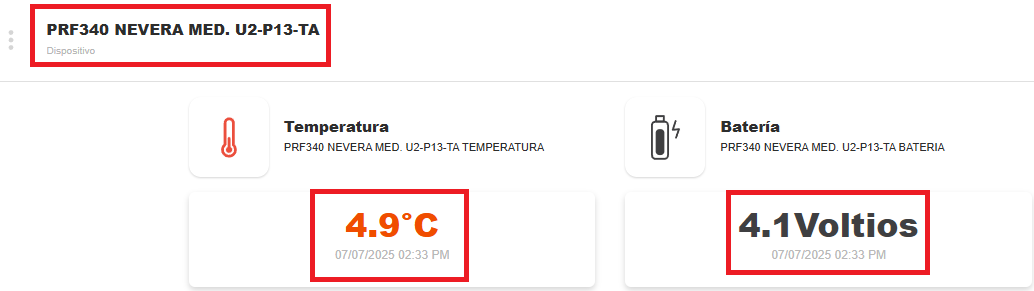
**Formato excel**

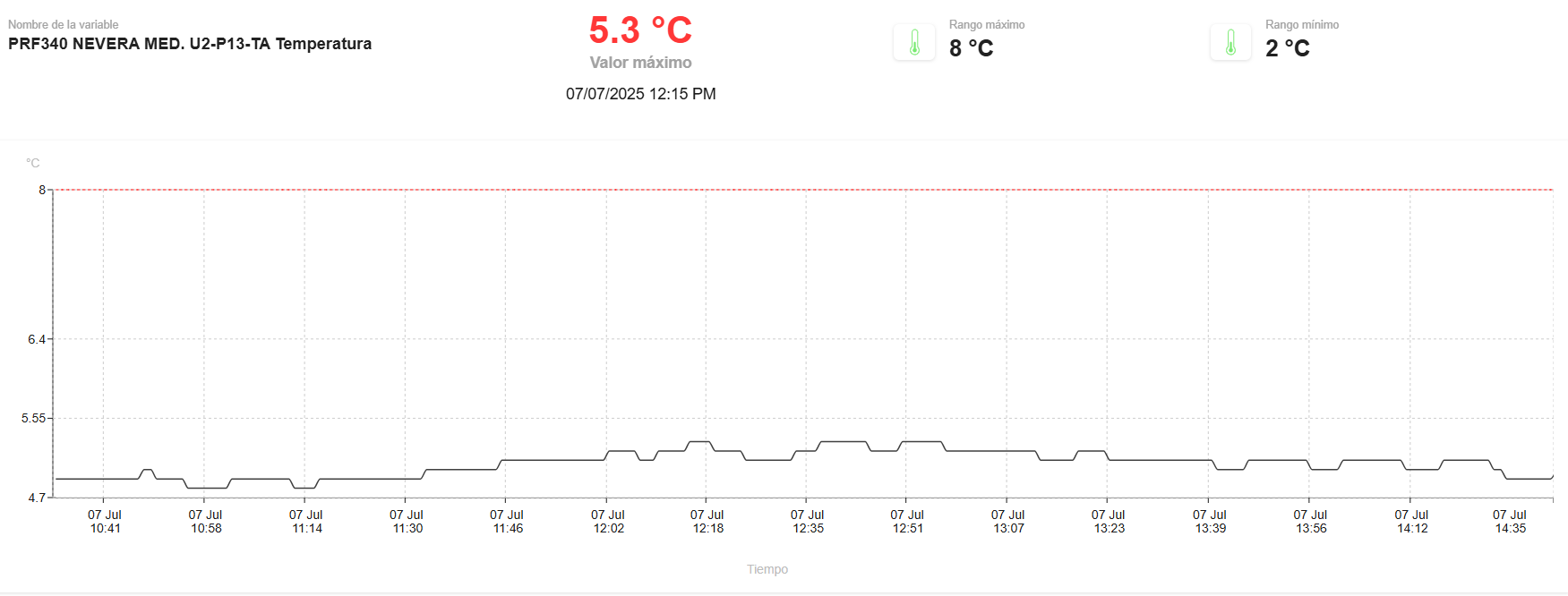


**Formato PDF**

* **Dashboards**

Son casillas que permiten ver el ultimo valor tomado por el sistema de monitoreo





1. **Menú de selección**

La solución desarrollada por Netux contiene un menú basado en UX (experiencia de usuario), el cual permite de una manera sencilla seleccionar cualquiera de las opciones entregadas en la solución.

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

* Dispositivos En esta sección de la plataforma aparece el listado de dispositivos con los que la entidad cuenta, donde se pueden visualizar los siguientes campos:
* Nombre de cada equipo
* Tipo de tecnología instalada
* Tipo de sensor del cada equipo
* Fecha de producción
* Versión del firmware de cada equipo

Interfaz de usuario gráfica, Aplicación, Teams

El contenido generado por IA puede ser incorrecto.

* Variables

En esta sección de la plataforma se pueden evidenciar todas las variables asociadas a cada equipo con los que cuenta la entidad. Además, nos permite visualizar de forma rápida los rangos de operación con los que cuenta cada dispositivo.

Imagen que contiene entero, rebaño, llenado, pájaro

El contenido generado por IA puede ser incorrecto.

* Contactos

En esta sección es posible visualizar los contactos que se tienen previamente configurados para la entidad, según la información y necesidad de cada una.

Interfaz de usuario gráfica, Aplicación, Teams

El contenido generado por IA puede ser incorrecto.

* Grupos: Dentro de esta sección, la plataforma permite:
* Agrupar diferentes dispositivos que cada entidad decida según la necesidad.
* Asociar a usuarios específicos en grupos puntuales, por ejemplo: los usuarios de la Sede 1 puede ver sólo la información correspondiente a la Sede 1.

Imagen que contiene Sitio web

El contenido generado por IA puede ser incorrecto.

1. **Eventos (envío de notificaciones)**

El sistema de monitoreo Netux, permite dar aviso de alarmas y precauciones por medio de SMS y/o correos electrónicos.

* **SMS**

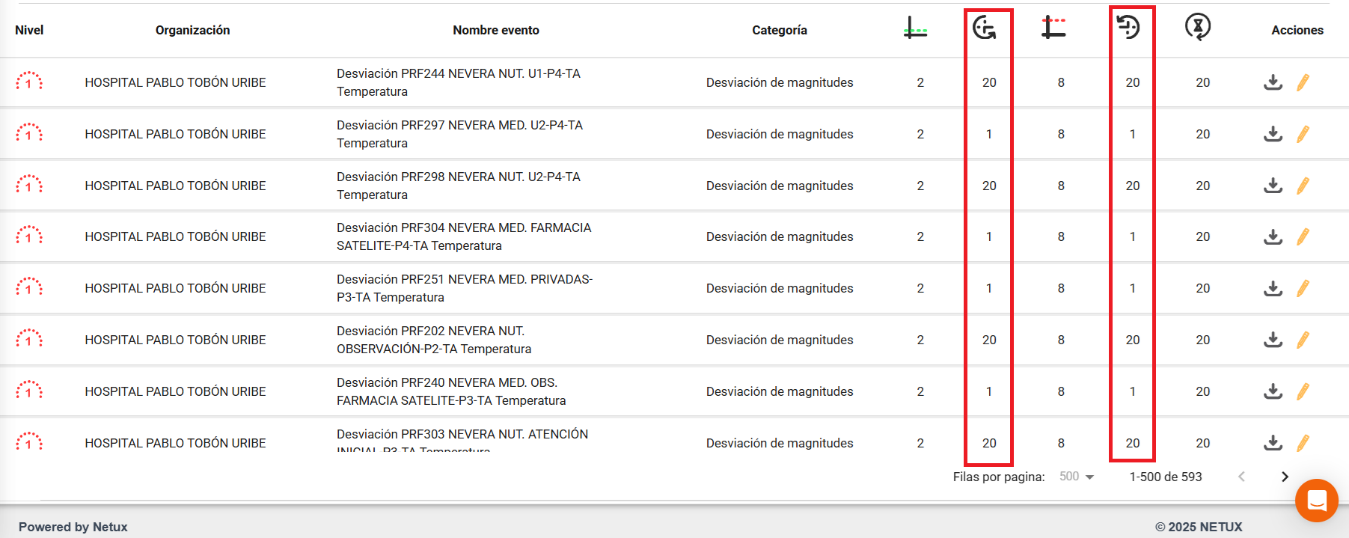
El servicio de mensajería de texto o SMS es configurado por NETUX SAS a los celulares que el cliente decida, las características técnicas de los SMS son las siguientes:

* Cualquier operador celular (Tigo, Comcel, Movistar)
* 3 usuarios
* **Correo electrónico**

El servicio de correo electrónico es configurado por Netux SAS a los usuarios que el Cliente decida, las características técnicas de los correos son las siguientes:

* Cualquier servidor de correo (gmail, hotmail, yahoo, propietarios, etc)
* Mensajes ilimitados
* 3 usuarios
* **Generación de notificaciones**

Las alarmas por desviación de magnitudes en neveras se envían al minuto de que la temperatura se encuentra fuera del rango establecido y se repiten cada 20 minutos en caso de que la desviación persista.



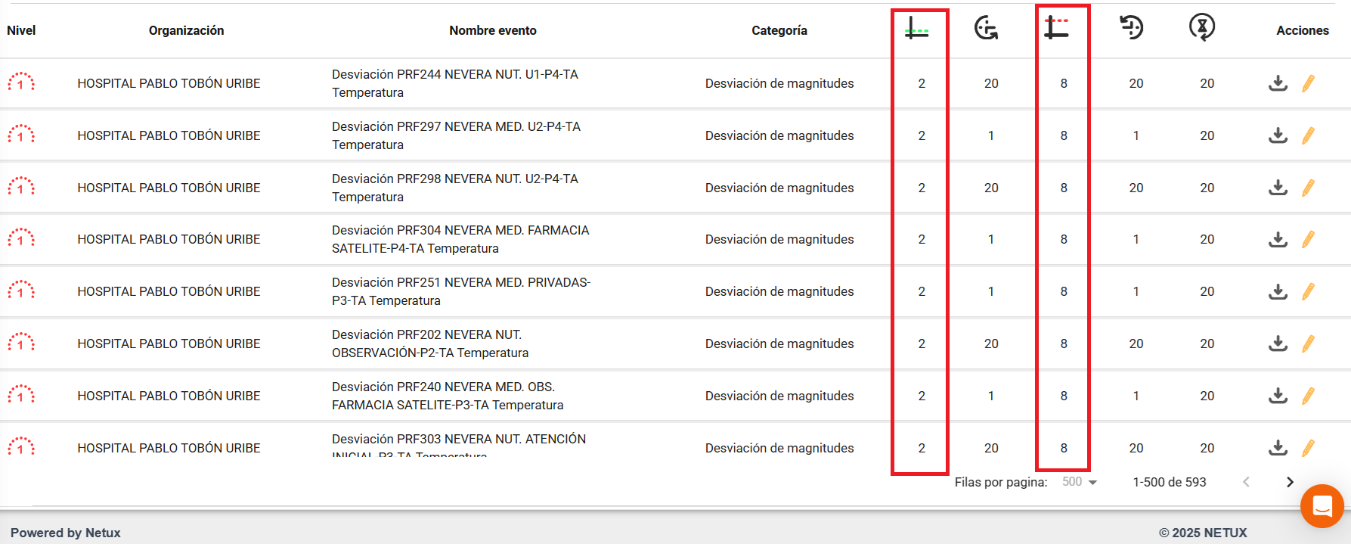
* **Formato y estados**

Todos los mensajes de la plataforma son enviados con el formato:

* Nombre de Variable en estado de alarma
* Fecha
* Valor

Los estados del sistema de telemetría poseen las siguientes características:

* Sobrepaso de límite superior e inferior
* Estos valores pueden ser configurados a cualquier valor o límite de tiempo.
* Cumpliendo con las condiciones “fuera de límites” y “tiempo mayor” al establecido es: denominado “alarma”



1. **Generación de reportes**

Dentro de esta sección está permitido realizar las siguientes funcionalidades por parte del usuario:

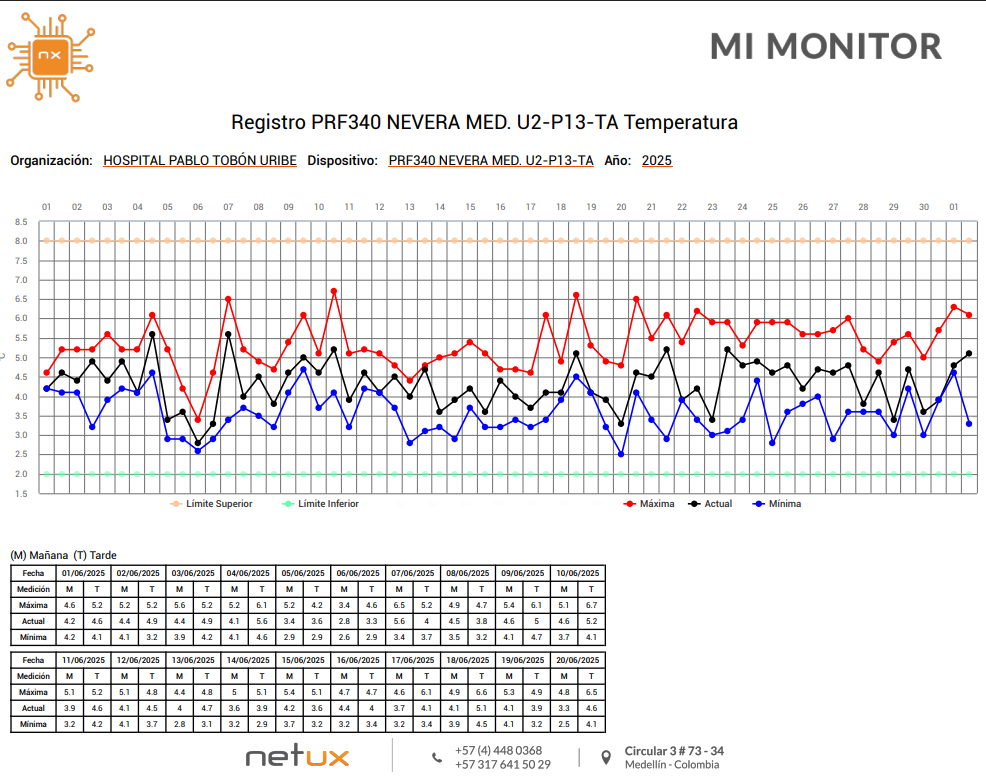
* Descarga de reporte gráficos PDF con máximos y mínimos.
* Descarga de reporte de valores de las variables
* Descarga de reporte de valores máximos y mínimos.



**Reporte de gráficos**

Este módulo permite tener acceso a un informe en pdf, que contiene la información gráfica del comportamiento de la cadena de frío registradas en tres tipos de informe diferentes que varían en función del tiempo de información requerido.

* Tipo 1(semana de información)
* Tipo 2 (15 días de información)
* Tipo 3 (1 mes de información)



Tabla

El contenido generado por IA puede ser incorrecto.

El reporte gráfico me permite sintetizar la información del periodo descargado en 3 gráficos: Temperatura Máxima, Temperatura mínima y Temperatura actual. Para la temperatura máxima y mínima, el reporte grafica durante la jornada de la mañana (M) comprendido entre las 00:01 y las 11:59 el valor máximo y mínimo correspondiente; en la jornada de la tarde (T) comprendido entre las 12:00 y las 23:59 el valor máximo y mínimo correspondiente.

Así mismo, la temperatura actual, me permite graficar la información en la jornada de la mañana (M) comprendida al valor más cercano de las 07:00 y la jornada de la Tarde (T) comprendida en el valor más cercano de las 17:00

**Reporte de valores**

La plataforma permite generar un tipo de informe, que consiste en todos los valores con las respectivas fechas, en un intervalo de tiempo definido por el usuario. Este informe es descargable en formato PDF o Excel.

Interfaz de usuario gráfica, Aplicación, Tabla, Excel

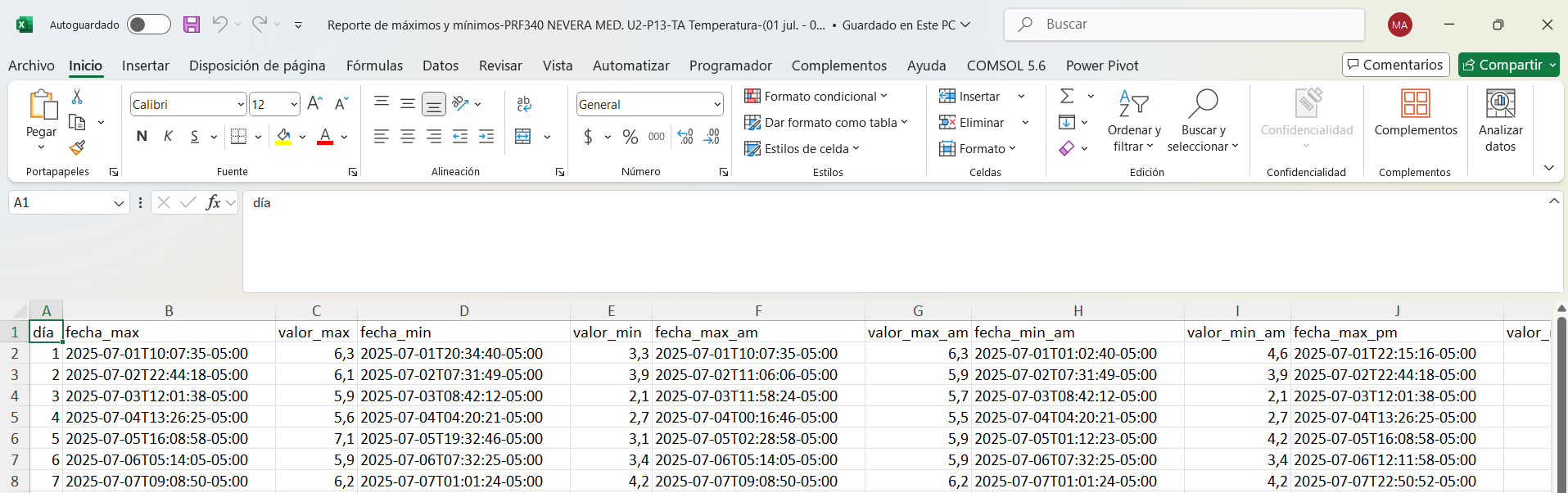
El contenido generado por IA puede ser incorrecto.

Tabla

El contenido generado por IA puede ser incorrecto.

**Reporte de máximos y mínimos**

La plataforma del sistema telemetría cuenta con un informe de auto gestión, que permite evaluar de manera periódica y controlada el reporte de actividad de la trazabilidad de la información máxima y mínima de la información registrada por nuestros sistemas, lo que hace posible llevar un resumen puntual del comportamiento diario a través del registro de valores máximos, mínimos y promedios. Estos informes pueden ser generados por fechas y son seleccionables por el usuario. Para ver instrucciones de uso de los informes favor remitirse al Documento *manual de usuario*.



1. **Acceso plataforma web**

La plataforma web para el monitoreo puede ser visualizada desde cualquier lugar del mundo con acceso a internet.



La plataforma web para el monitoreo puede ser visualizada, desde los navegadores:

Un dibujo de un perro

Descripción generada automáticamente con confianza media

El ingreso a la plataforma de telemetría se hace a través del link:

<https://mimonitor.netuxcloud.com/>

1. **Conexión equipo de telemetría – Internet**

**10.1 Etapa de comunicación**

La etapa de comunicación se hace a través de internet asignando protocolos de seguridad y conexiones al servidor de la plataforma WEB. El protocolo utilizado es el HTTPS explicado anteriormente en la sesión *‘seguridad’.*

**Flujo de Operación de Nx sensor Pro / Lite**

El monitor de temperatura toma datos de forma continua por medio de un transductor (sensor) de temperatura, Temperatura. El sensor es de tipo digital y se encarga de analizar la magnitud física del entorno. Estos datos son capturados por el módulo de procesamiento del registrador de datos, el cual se encarga de acondicionar las señales eléctricas de corriente de forma que puedan ser interpretadas para el usuario final en función de unidades de medida de °C una vez enviadas a la plataforma del sistema informático.

**Transductor**



**Transductor**

**Registrador datos**

**10.2 Proceso de transmisión**

El dispositivo abre la conexión con el servidor alojado en la dirección física API.UBIDOTS.COM a través del puerto 443 o (puerto para el HTTPS).

Diagrama

Descripción generada automáticamente



Una vez establecido el enlace de comunicación, cada dispositivo se identifica mediante un TOKEN, el cual actúa como una llave electrónica única e intransferible asignada a cada equipo. Este mecanismo de autenticación garantiza que únicamente el equipo autorizado sea el que transmite la información. Ningún otro dispositivo en el mundo puede replicar esta transmisión, asegurando así la fidelidad, autenticidad y trazabilidad del dato registrado por los monitores.

**Modelo Nx Sensor Pro**

Para la transmisión de información hacia la nube, el modelo Nx Sensor Pro dispone de un canal de comunicación independiente basado en tecnología Quad-Band 4G LTE y GSM, lo cual le permite operar de forma autónoma. El equipo registra datos de forma continua en intervalos de 1 minuto, y los transmite utilizando el protocolo estándar GPRS sobre redes celulares.

No obstante, es importante aclarar que factores externos al funcionamiento del equipo —como condiciones ambientales, estabilidad del canal de comunicación o intensidad de señal en la zona— pueden afectar momentáneamente la transmisión, generando posibles retardos en el envío de datos de entre 1 y 3 minutos.

**Modelo Nx Sensor Lite**

En el caso del modelo Nx Sensor Lite, la transmisión de datos hacia la nube se realiza a través de un canal de comunicación local, que permite enviar la información a un dispositivo intermedio denominado Gateway. Este Gateway actúa como centralizador de datos y cuenta con su propio canal de comunicación autónomo Quad-Band 4G LTE y GSM, permitiendo la posterior transmisión hacia la nube.

A diferencia del modelo Pro, el intervalo de actualización del sistema para los datos capturados por el Nx Sensor Lite es de 5 minutos, debido a su arquitectura distribuida y modelo de transmisión indirecta.

**10.3 Enfoque basado en riesgo**

La gestión del riesgo es un proceso sistemático que busca asegurar, comunicar y controlar los riesgos asociados a la seguridad de la información, calidad del producto e integridad de los datos.

Este análisis considera lo siguiente:

• Identificar el riesgo.

• Análisis del riesgo cualitativo.

• Evaluación del riesgo (detección, severidad y ocurrencia)

• Seguimiento y revisión

**Tabla 1.** Especificaciones funcionales para la validación del sistema informático

|  |  |  |
| --- | --- | --- |
| **Especificaciones funcionales** | | |
| **Número** | **Descripción** | **Categoría** |
| 1 | Registro de valores de magnitudes físicas (°C, %HR) | O |
| 2 | Registro de datos en tiempo real | O |
| 3 | Autenticación de usuario y contraseña | O |
| 4 | Back up de datos y actualización de registros del sistema | O |
| 5 | Visualización de datos a través de gráficas, dashboard y variables | D |
| 6 | Interfaz de usuario: menú de selección | D |
| 7 | Eventos (Envío de notificaciones) | O |
| 8 | Generación de reportes | D |
| 9 | Acceso plataforma web | D |

\*Obligatorio: O, Deseado: D

Después de tener establecidas las especificaciones funcionales se procederá con el análisis de riesgos bajo el modelo de *ICH Q9 FMEA* para los requisitos obligatorios, de la siguiente manera:

**Tabla 2.** Asignación de riesgo a cada especificación funcional

|  |  |  |  |
| --- | --- | --- | --- |
| **Especificaciones funcionales (Legales)** | | | |
| **Número** | **Descripción** | **Número del riesgo** | **Descripción del riesgo** |
| 1 | Registro de valores de magnitudes físicas (°C, %HR) | 1 (R1) | Los valores registrados de variables físicas (como °C y %HR) son susceptibles de modificación manual |
| 2 (R2) | Falta de veracidad en el registro de valores de magnitudes físicas |
| 2 | Registro de datos en tiempo real | 3 (R3) | Registro no permanente de datos |
| 3 | Autenticación de usuario y contraseña | 4 (R4) | Acceso no autorizado al sistema |
| 4 | Back up de datos y actualización de registros del sistema | 5 (R5) | Pérdida total o parcial de datos críticos debido a la ausencia, falla o mala configuración del sistema de respaldo, o errores durante la actualización del sistema |
| 5 | Eventos (Envío de notificaciones) | 6 (R6) | El sistema no genera eventos o alertas ante desviaciones de parámetros críticos (°C, %HR) respecto a los rangos establecidos |

**Tabla 3. Criterios de evaluación**

|  |  |  |  |
| --- | --- | --- | --- |
| **Escala** | **Severidad** | **Ocurrencia** | **Detección** |
| 1-3 | Menor impacto en calidad | Rara vez ocurre | Muy alta capacidad de detección |
| 4-6 | Impacto moderado (reproceso) | Posible, pero no frecuente | Moderada capacidad de detección |
| 7-8 | Afecta cumplimiento GxP | Ocurre ocasionalmente | Detección limitada |
| 9-10 | Riesgo crítico (producto inseguro, pérdida de trazabilidad) | Frecuente o constante | Muy baja o nula capacidad de detección |

**Tabla 4.** Análisis y evaluación de riesgos

|  |  |  |  |
| --- | --- | --- | --- |
| **Número**  **del riesgo** | **Severidad** | **Probabilidad de ocurrencia** | **Probabilidad de detección** |
| R1 | 10 | 1 | 9 |
| R2 | 10 | 1 | 1 |
| R3 | 8 | 6 | 1 |
| R4 | 4 | 3 | 7 |
| R5 | 10 | 1 | 1 |
| R6 | 10 | 1 | 1 |

**Tabla 5**. Evaluación del riesgo severidad Vs. Probabilidad de ocurrencia

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Severidad** | **Evaluación del riesgo** | | | | |
| **9-10** | **R1, R2, R5, R6** |  |  |  |
| **7-8** |  | **R3** |  |  |
| **4-6** | **R4** |  |  |  |
| **1-3** |  |  |  |  |
|  |  | **1 - 3** | **4-6** | **7-8** | **9-10** |
|  |  | **Probabilidad ocurrencia** | | | |

**Tabla 6.** Evaluación del riesgo severidad Vs. Probabilidad de detección

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Severidad** | **Evaluación del riesgo** | | | | |
| **9-10** | **R2, R5, R6** |  |  | **R1** |
| **7-8** | **R3** |  |  |  |
| **4-6** |  |  | **R4** |  |
| **1-3** |  |  |  |  |
|  |  | **1 - 3** | **4-6** | **7-8** | **9-10** |
|  |  | **Probabilidad detección** | | | |

**Tabla 7**. Clasificación del riesgo

|  |  |
| --- | --- |
|  | Riesgo minimo |
|  | Riesgo medio |
|  | Riesgo alto |

Los riesgos que sean calificados como críticos serán objeto de análisis y verificación durante la validación:

ICH Q9 recomienda que los riesgos con NPR (Número de prioridad de riesgo) superiores a 100 sean objeto de acciones de mitigación prioritaria. El análisis debe ser documentado y revisado periódicamente durante el ciclo de vida del sistema (incluyendo DQ, IQ, OQ, PQ).

Esta evaluación permite tomar decisiones basadas en riesgo, asegurando el cumplimiento GxP y la integridad del producto o servicio.

**REFERENCIACIÓN NORMATIVA PARA EL PROCESO**

* *GAMP 5: Risk-Based Approach to Compliant GxP Computerized Systems, International Society for Pharmaceutical Engineering(ISPE),2008, United states.*
* *Colombia. Ministerio de la Protección Social. (2009). N° 6, Articulo 6 RESOLUCIÓN 4410 DE 2009*

**INFORME DE DESVIACIONES**

Desviación (es):

No aplica

Justificación de la aceptación:

No aplica

Impacto sobre la operación, función o proceso:

No aplica

|  |  |
| --- | --- |
| **Realizó desviación** | N/A |
| Fecha: No aplica |
| **Verificó desviación** | N/A |
| Fecha: No aplica |

**INFORME DE CALIFICACIÓN DE ESPECIFICACIONES FUNCIONALES**

**Resultados:**

Todos los datos consignados en el presente informe respaldan el adecuado funcionamiento del sistema de telemetría implementado en el {{nombre\_establecimiento}}. La información documentada ha sido verificada y es soportada técnicamente por la empresa Netux, en calidad de proveedor y responsable del sistema.

**Conclusiones:**

Con base en los resultados obtenidos durante la ejecución del protocolo de calificación en sitio, se puede concluir que la solución de telemetría implementada en el {{nombre\_establecimiento}} ha sido validada satisfactoriamente. Se evidenció de manera documental el correcto funcionamiento del sistema informático destinado al registro continuo de datos de variables físicas, cumpliendo con los requisitos definidos previamente y garantizando la conformidad con las condiciones establecidas en el presente informe.

Este resultado respalda la liberación del sistema para su uso en operación rutinaria, en cumplimiento con los lineamientos de buenas prácticas de gestión de datos y conforme a lo estipulado por los marcos normativos aplicables

|  |  |
| --- | --- |
| **Realizó** | {{nombre\_realizo}}anci |
| Fecha: 07/07/2025 |
| **Verificó** | Ruben Darío Tabares |
| Fecha: 08/07/2025 |
| **Aprobó** | Daniel Antonio Quintero Rincón |
| Fecha: 11/07/2025 |